IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KARIM KHOWAJA, individually and on behalf of all similarly situated individuals, *Plaintiff*, v. ADIDAS AMERICA, INC., an Oregon corporation, *Defendant*.	)	No. 25-cv-06154 Hon. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Karim Khowaja ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint against Defendant Adidas America, Inc. ("Defendant") as a result of Defendant's actions and inactions concerning a recent data breach that compromised the personally-identifiable information ("PII") of Plaintiff and other members of the putative class. Plaintiff alleges as follows based on personal knowledge as to his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

INTRODUCTION

1. Plaintiff brings this class action lawsuit against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' PII from unauthorized third parties.

2. On or about May 30, 2025, Defendant informed Plaintiff and other customers that their PII, including at a minimum their names, email addresses, telephone numbers, genders, and birth dates, had been breached through one of Defendant's third-party customer service providers.

Defendant's "disclosure" amounts to no real disclosure at all as it failed to inform affected individuals of the data breach's critical facts, leaving victims with little ability to mitigate the breach's adverse effects. Defendant has refused to disclose the identity of the affected customer service provider or disclose in any detail how or when the breach occurred.

3. Defendant is the American affiliate of one of the largest athletic apparel brands in the world. Major retailers such as Defendant collect a treasure-trove of information from their customers, and have an obligation to employ reasonable and necessary data security practices – including on the part of their third-party customer service contractors – to protect the confidential and personal information entrusted to them.

4. This duty exists because it is foreseeable that the exposure of such private information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, spam calls, phishing attacks, financial identity theft, and other long-term issues.

5. The harm resulting from a data and privacy breach manifests in several ways, including identity theft and financial fraud, and the exposure of a person's private through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

6. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time, money and other resources to closely monitor their credit accounts, email accounts, and online accounts with other companies, as well as to take a number of additional preventative measures.

7. Plaintiff and the Class members are now at an increased and certainly impending risk of fraud, identity theft, and similar forms of criminal mischief, risks which may last for the rest of their lives.

8. Consequently, Plaintiff and the Class members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes. *See McMorris v. Lopez*, 995 F.3d 295, 301 (2d Cir. 2021) (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to . . . assumer those consumers' identities").

9. Plaintiff brings this action to remedy the violation of his privacy rights due to Defendant's actions and inactions resulting in the data breach as well as Defendant's breach of its implicit agreement to safeguard his PII. Defendant's negligent and reckless conduct has led to a release of Plaintiff's PII that, in addition to being a breach of privacy, puts him at risk of targeting by nefarious, sophisticated, and financially-motived actors.

10. To this day, Plaintiff continues to rely on his own time, efforts, and expense to monitor and assess the extent to which his valuable PII was compromised and will continually monitor his accounts into the foreseeable future.

11. On behalf of himself and the proposed Class defined below, Plaintiff seeks monetary and equitable damages, together with costs and reasonable attorneys' fees.

PARTIES

12. At all relevant times, Plaintiff has been a resident and a citizen of the state of Illinois.

13. Defendant Adidas America, Inc. is a corporation organized under the laws of the state of Oregon with its principle place of business located in Portland, Oregon.

JURISDICTION AND VENUE

14. This Court has diversity jurisdiction under 28 U.S.C. § 1332(d), because (i) at least one member of the putative class is a citizen of a state different from any Defendant, (ii) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (iii) none of the exceptions under that subsection apply to the instant action.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), because Defendant transacts business in this District, and because a substantial part of the events giving rise to Plaintiff's claims occurred in this District, as Plaintiff had his PII collected and used by Defendant in this District.

COMMON FACTUAL ALLEGATIONS

16. Defendant sells athletic apparel and footwear in brick-and-mortar stores across the United States as well as through its website, adidas.com.

17. As part of its online sales, Defendant collects a host of information from prospective customers, including their identity, contact, and other demographic information, their payment information, and their browsing and website behavior.

18. At the same time, Defendant has touted its data security practices. For instance, Defendant tells prospective customers that "you shouldn't order from a company that doesn't follow reasonably secure data practices. We use reasonable security procedures to protect your information." With respect to its third-party service providers, Defendant claims that such providers – including its customer service vendors – "are contractually obligated to maintain the

confidentiality and security of your information. They are subject to appropriate contractual restrictions on how they use this information."[1]

19. Nonetheless, as demonstrated by the breach of Plaintiff's and other individuals' PII, Defendant does not maintain reasonable security procedures or ensure that its third-party service providers do either.

20. Indeed, Defendant should have expected this exact result stemming from its deficient data security practices, because its customers' private information has been breached before. In 2018, for instance, Defendant was forced to acknowledge that millions of its customers' contact information, usernames, and passwords were breached due to a security vulnerability. *See Adidas Breach Impacts Millions of US Customers*, FORTRA (Jul. 2, 2018), available at https://www.digitalguardian.com/blog/adidas-breach-impacts-millions-us-customers.

21. Thus, Defendant must have known that a breach of its systems, or a breach of its third-party service providers' systems, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

22. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce." *See The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), available at https://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

23. The more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique

[1] https://www.adidas.com/us/help/us-company-information/what-is-the-privacy-policy (last visited June 2, 2025).

referred to as "social engineering" to obtain even more information about a victim's identity by targeting them with spam calls and texts or phishing attacks.

24. Thus, even if certain information was not purportedly involved in the latest breach of Defendant's customers' PII, the unauthorized parties could use their PII to access other accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity.

25. In light of these risks, the Federal Trade Commission has published numerous cybersecurity guidelines for businesses discussing the "significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII" and how different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[2]

26. Notably, the FTC has explained that "your company's security practices depend on the people who implement them, including contractors and service providers . . . Put your security expectations in writing in contracts with service providers. Then, don't just take their word for it—***verify compliance***."[3]

27. As demonstrated by the breach of Plaintiff's and other customers' PII, Defendant failed to undertake these most basic of data security measures.

---

[2] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, FED. TRADE COMM'N 35–38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[3] *Protecting Personal Information, A Guide for Business*, FED. TRADE COMM'N 27 (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (emphasis added).

28. Defendant's failure to comply with reasonable data security standards, failure to use secure systems, and/or failure to ensure its service providers used secure systems provided Defendant a benefit in the form of saving on the costs of compliance, but at the expense of and severe detriment to its customers, including Plaintiff and the other Class members, whose PII has been exposed in the data breach or otherwise placed at serious and ongoing risk of imminent misuse, fraudulent charges, and identity theft

PLAINTIFF'S EXPERIENCE

29. Plaintiff has purchased multiple athletic apparel items from Defendant. In connection with his purchases, Plaintiff was required to provide Defendant with his PII, including his first and last name, birth date, email address, gender and phone number.

30. Plaintiff provided his PII to Defendant with the understanding and belief that his information would be reasonably secured.

31. On May 30, 2025, Defendant sent Plaintiff an email notifying him that his PII had been breached, purportedly "through a third-party customer service provider," though Defendant failed to identify the provider or provide any other information regarding the breach.

32. As a direct result of Defendant's inadequate data security measures, Plaintiff has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

33. On information and belief, Plaintiff's PII was unauthorizedly disclosed in the breach and is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

34. In addition, Plaintiff must now spend time and effort attempting to remediate the harmful effects of the breach, including monitoring his credit reports, and fears for his personal

financial security and uncertainty over the information compromised in the data breach. He is experiencing feelings of anxiety and fear because of the breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

35. Since recently becoming aware of the data breach, Plaintiff has taken time dealing with increased spam calls and emails, monitoring irregularities in his credit reports, and otherwise mitigating his risk of identity theft and fraud, including monitoring his virtual accounts to guard against fraudulent attempts to open accounts in his name.

36. Plaintiff has also been harmed by having his PII compromised and faces the imminent and impending threat of future additional harm from the increased threat of identity theft and fraud due to his PII being sold, misappropriated, or otherwise misused by unknown parties.

CLASS ALLEGATIONS

37. Plaintiff brings this action individually and on behalf of the following class ("the Class") pursuant to Rules 23(a) and 23(b) of the Federal Rules of Civil Procedure:

> **Class:** All individuals in the United States whose PII was compromised in the data breach announced by Defendant in May 2025.

38. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

39. Upon information and belief, there are thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of Class members is currently unknown to Plaintiff, the precise size of the Class may easily be ascertained through Defendant's records.

40. Plaintiff's claims are typical of the claims of the Class members he seeks to represent because the factual and legal bases of Defendant's liability to Plaintiff and the other Class members are the same and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class members. As alleged herein, Plaintiff and the other Class members have all suffered damages as a result of Defendant's failure to maintain reasonable security safeguards with respect to its handling of its customers' sensitive information.

41. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant had a duty to protect the PII of Plaintiff and the Class members;

b. Whether Defendant adequately safeguarded Plaintiff's and the Class members' PII;

c. Whether Defendant entered into an implied contract with Plaintiff and the Class members;

d. Whether Defendant breached that contract by failing to adequately safeguard Plaintiff's and the Class members' PII;

e. Whether Defendant was unjustly enriched; and

f. Whether Plaintiff and the Class members are entitled to damages and other relief as a result of Defendant's wrongful conduct.

42. Absent a class action, most Class members would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

43. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other Class members and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

44. Defendant has acted and failed to act on grounds generally applicable to Plaintiff and the other Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Class)

45. Plaintiff realleges the foregoing allegations as if fully set forth herein.

46. At all relevant times, Defendant had a duty, or undertook/assumed a duty, to implement reasonable data privacy and cybersecurity protocols, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of the Plaintiff and the Class members, *i.e.* to utilize secure systems and ensure the security of its service providers' systems, and to prevent the unauthorized access to and disclosures of the same. This duty included, among other things, designing, implementing, maintaining, and testing Defendant's and/or its service providers' cybersecurity systems to ensure that Plaintiff's and the Class members' PII was reasonably secured and protected.

47. For example, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities

such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

48. In addition, due to Defendant's position as a business invitor and position of exclusive control, knowledge, and discretion regarding its cybersecurity practices compared to Plaintiff's and other customers' relative lack of power concerning the same, a duty arose due to such special relationship that required Defendant to implement adequate cybersecurity protocols regarding its technical, administrative, and physical controls.

49. Defendant breached the aforementioned duties in, including but not limited to, one or more of the following ways:

A. Failing to implement reasonable data privacy and cybersecurity measures to secure Plaintiff's and Class members' information;

B. Failing to implement reasonable measures to verify its third-party service providers' data privacy and cybersecurity measures;

C. Failing to evaluate and adjust its data security protocols following prior instances of the breach of its customers' PII;

D. Failing to follow its own privacy policies and practices published to prospective customers; and

E. Otherwise failing to act reasonably under the circumstances and being negligent with regards to their conduct in preventing, detecting, and disclosing the data breach.

50. Further, Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII by not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving its customers' PII.

51. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

52. As a direct and proximate result of Defendant's negligent acts and omissions, Plaintiff and the Class members have suffered actual injury and damages as expressed herein, including the loss of their legally protected interest in the confidentiality and privacy of their PII, the loss of the benefit of their bargain in receiving consumer goods from Defendant, pecuniary injury in the form of time and expense to mitigate the disclosure and/or significantly increased risk of exposure of PII to nefarious third parties.

53. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

54. Plaintiff realleges the foregoing allegations as if fully set forth herein.

55. Plaintiff and the Class members are parties to a contract implied-in-fact with Defendant whereby Defendant offered consumer goods and fulfillment services to Plaintiff and the Class members in exchange for consideration. The amount of such consideration included Defendant's provision of reasonable and adequate cybersecurity protections to prevent the unauthorized disclosure of Plaintiff's and the Class members' sensitive personal data.

56. Prior to receiving such consumer goods and services from Defendant, Plaintiff and the Class members provided their PII to Defendant, which Defendant accepted, received, stored, and otherwise handled in order to, *inter alia*, provide them goods and services for monetary consideration.

57. By accepting, receiving, storing, and handling Plaintiff's and the Class members' PII in order to provide them consumer goods and services in exchange for consideration, and by

virtue of Plaintiff and the Class members providing such PII in accordance with the same, a contract implied-in-fact was created by the aforementioned conduct of Plaintiff and the Class members, on the one hand, and Defendant with regard to the handling and management of such PII.

58. As part of these agreements, Defendant was paid for, and was obligated to implement, reasonable cybersecurity standards, including monitoring the cybersecurity standards of its customer service providers, in order to safeguard and prevent the unauthorized disclosure of Plaintiff's and Class members' PII.

59. Defendant's failure to implement adequate and reasonable data privacy and cybersecurity protocols which included ensuring that it and its service providers used systems that were secure, constitutes a breach of the contract implied-in-fact.

60. Plaintiff and the Class members would not have provided and entrusted their PII to Defendant or would have sought other alternative goods and services from Defendant's competitors, in the absence of an agreement with Defendant to reasonably safeguard their PII.

61. Plaintiff and the other Class members fully performed their obligations under their implied contract with Defendant, including by providing their PII and providing consideration.

62. Defendant's breach of its implied contracts with Plaintiff and the Class members caused them to sustain losses and damages including actual injury and damages as expressed herein, including the loss of their legally protected interest in the confidentiality and privacy of their PII, the loss of the benefit of their bargain in receiving consumer goods and services from Defendant, pecuniary injury in the form of time and expense to mitigate the disclosure and/or significantly increased risk of exposure of PII to nefarious third parties.

63. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

64. Plaintiff and the Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen its data security systems and monitoring procedures to prevent future breaches of their PII and (2) immediately provide and continue to provide adequate credit monitoring to Plaintiff and the Class members.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

65. Plaintiff realleges the foregoing allegations as if fully set forth herein.

66. Plaintiff brings this claim in the alternative to Count II above.

67. On information and belief, Defendant funds its data security measures from its general revenue including payments made by or on behalf of Plaintiff and the Class members.

68. As such, Defendant received a monetary benefit from Plaintiff and the Class members' purchase of Defendant's goods and services, in the form of monetary payment for such goods and services, including reasonable data security services.

69. Defendant accepted such monetary benefit but grossly failed to provide reasonable data and security services by failing to ensure the security of its systems and/or the systems of its service providers, which Defendant knew or should have known to be the target of cybercriminals, resulting in the breach of Plaintiff's and the Class members' PII.

70. Defendant knew that Plaintiff and the Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used Plaintiff's and the Class members' PII for business purposes.

71. Under principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit conferred upon it for reasonable data security services that it failed to provide.

72. Defendant acquired Plaintiff's and the Class members' PII through inequitable means by publicly stating that it and its service providers maintained reasonable data security protocols, when the opposite was true.

73. Accordingly, because Defendant will be unjustly enriched if it is allowed to retain such funds, Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that Defendant unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and the Class members overpaid for Defendant's goods and services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, respectfully requests that this Court enter an Order:

A. Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;

B. For equitable and injunctive relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiff's and the Class members' PII, and as necessary to protect the interests of Plaintiff and the Class members;

C. For an award of damages, including but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

D. Requiring Defendant to pay Plaintiff and the Class members' reasonable attorneys' fees, expenses, and costs;

E. Pre- and post-judgment interest on any amounts awarded; and

F. Any such further relief as this Court deems reasonable and just.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: June 2, 2025

Respectfully submitted,

KARIM KHOWAJA, individually and on behalf of similarly situated individuals

By: /s/ Timothy P. Kingsbury
One of Plaintiff's Attorneys

Timothy P. Kingsbury
KINGSBURY LAW LLC
8 S. Michigan Ave., Ste. 2600
Chicago, IL 60603
Tel: (312) 291-1960
tim@kingsburylawllc.com

Counsel for Plaintiff and the proposed Class